Modern Measures of Risk Reduction in Industrial Processes

Submitted: 8th October 2018; accepted 7th February 2019

Jan Maciej Kościelny, Michał Syfert, Bartłomiej Fajdek

DOI: 10.14313/JAMRIS_1-2019/3

Abstract:
The article describes standard safety-protection layers according to EN 61511 standard. Their aim is to reduce risk, thus to decrease the frequency of occurrence of threatening incidents and/or consequences of such incidents. The aim of the article was to present currently developed means of increasing process safety, which are not included in the standards. There are described: advisory diagnostic systems, fault tolerant control systems, process simulators for operators training and IT systems supporting safety. Such components can be treated as additional layers of process protection. A simple example comparing the operation of alarm and diagnostic systems as well as the example of the fault tolerant control system of the level in the drum boiler in sugar factory are given.

Keywords: *risk reduction, layers of protection, real-time diagnostic systems, fault tolerant control systems, process simulators*

1. Introduction

Technical safety is considered in two ways, safety as a problem of prevention against serious industrial accidents caused by unreliability of components of technological installation, such as pipeline breaks, faults of the elements of control systems and human errors; another aspect is security understood as an issue of protection against intentional, unfriendly external attacks, e.g. hacker attacks on control systems [11, 2, 13], and internal sabotage actions [17]. This paper analyses only the first aspect of safety.

The risk of serious industrial accidents is at the moment one of the most important threats occurring in highly developed countries [35, 33, 23, 21]. A significant element of preventing such accidents is an issue of early detection and elimination of the sources of potential risks. For all installations posing a risk to human life or health, as well as to the environment and property, existing legal regulations and technical standards introduce a requirement of ensuring appropriate level of safety, i.e. reducing the risk to the acceptable level [17, 22, 14, 27, 31]. Direct impulse for developing and adopting directives on preventing serious industrial accidents was a Seveso disaster, which in consequence led to developing 3 other directives on risk control and reduction.

An important element of technical safety is functional safety referring to all actions in the operating cycle of systems made of electric and/or electronic and/or electronically programmed components. International action standards aimed at ensuring safety are defined through the following standards, as regards: general rules of functional safety – EN 61508 [38], industrial processes – EN 61511 [39], machines – EN 62061 [40] and nuclear power – EN 61513 [41].

The aim of this paper is a brief characteristics of currently developed measures increasing safety of the processes, which are not included in the above-mentioned standards. We presented diagnostic expert systems, fault tolerant control systems, process simulators for operators training and computer systems supporting safety. These elements can be treated as additional layers of protection for the processes.

2. Standard Layers of Protection

The aim of safety systems is risk reduction, thus minimizing the frequency of risk posing incidents and/or the reduction of their consequences. The structure of the used safety systems is layered (Fig. 1).

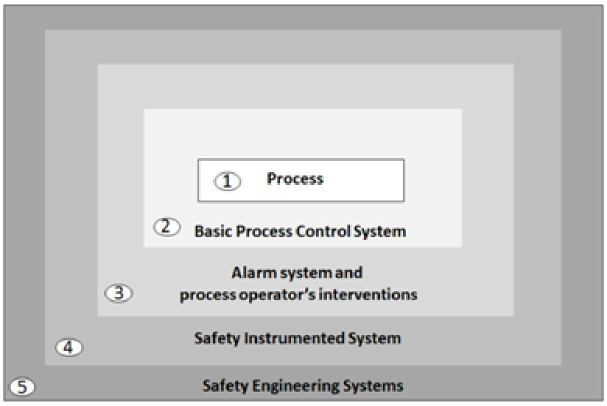
① Process
② Basic Process Control System
③ Alarm system and process operator's interventions
④ Safety Instrumented System
⑤ Safety Engineering Systems

Fig. 1. Typical layers of protection

The first layer is process installation, which should be resistant to internal and external interferences. The second layer is a Basic Process Control System, such as DCS (Distributed Control Systems), where control and monitoring is integrated, or system made of SCADA (Supervisory Control and Data

Acquisition) and Programmable Logic Controllers or Programmable Automation Controllers. Third layer is a separate system of critical alarms and interventions of process operators. Safety Instrumented Systems (SIS) constitute a fourth layer. These four layers are responsible for preventing the occurrence of accidents. Fifth layer is engineering safety systems, such as safety valves, curtains, safety barriers, housing etc., which are supposed to limit the consequences of the accidents. The higher layers are internal and external procedures and technical means aimed at minimizing human and material losses.

2.1. Process Installation

The first layer is process installation, which should be resistant to internal and external interferences. When designing technical installations one should aim to eliminate or reduce possible emergency scenarios. The object should be characterized by intrinsic safety [4], i.e. embedded in its construction. As an example, there are efforts to introduce new technologies of nuclear reactors, which will provide maximum work safety and minimize the effects of possible accident. Their aim is to eliminate an opportunity of a core melt-down and the release of nuclear fission products outside the reactor. Unfortunately, in most cases it is not possible to design an installation in such a way to eliminate all potential risks, thus the other layers of protection are necessary.

2.2. Basic Process Control System

Second layer is Basic Process Control System in the form of DCS (Distributed Control Systems), where the control and monitoring is integrated [15, 30, 32], or system made of SCADA (Supervisory Control and Data Acquisition) and Programmable Logic Controllers or Programmable Automation Controllers. Their aim is sustaining the process in a normal condition in all their stages – start, normal exploitation and stopping. Stabilization of pressures, flows, levels, temperatures etc. usually doesn't lower the risk, because the set values of regulation systems are selected in the area of safety states. In the case of optimal control the risk usually increases due to the fact of conducting processes close to safety limitations, where optimal operating points are usually located.

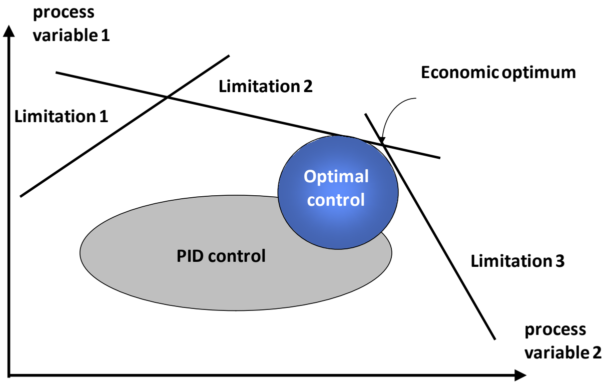

Fig. 2. The operation areas of PID and optimization algorithms

However, it should be emphasized that regulation systems are not resistant to the faults of drivers, measuring devices and actuators. Redundancy is mostly used for drivers, which are damaged least often. If we consider only accidents caused by control systems, then, according to the data from ABB and Emerson companies and ASM (Abnormal Situation Management) consortium, about 50% of them is caused by the damage to the actuators, 40% to measuring devices and only 10% to control units. Damages to the actuators, as well as measuring circuits were the reason of serious industrial accidents, e.g. in Buncefield in England in December 2005 [43]. Breakdown of level sensor in oil storage facility caused overflow, and then an explosion. This was the biggest fire in Europe, 40 people were injured and material losses were estimated at 5 billion pounds.

We have to stress one more feature of regulation systems, the operation of negative feedback loop results in masking the symptoms of faults. As an example, a leak of toxic substance from the tank with an active regulation system of a fixed value level may not be detected by the alarm system due to the increase of inflow of medium to the tank through a regulator [15]. The situation is presented in Fig. 6.

2.3. Alarm Systems and Operators Action

In SCADA and DCS systems, as well as in SIS, alarm system (AS) is used for detecting abnormal and emergency states. Basic method of fault detection used in AS is limitation control [9, 16, 15, 18]. With the use of this method, exceeding of the absolute and relative (referring to the set point) limitations are detected by process variables. Limitations concern the value, and also the allowed speed of signal changes.

In a well-designed AS, every alarm should be useful and significant for the operator, i.e. it should warn, inform and indicate appropriate reaction. In practice, this requirement is hardly ever fulfilled. The basic disadvantage of AS is an excess of the generated alarms. From the data gathered by EEMUA [7] it turns out that an average daily number of alarms in petrochemical industry is 1.500 and in the power industry – 2.000, whereas, according to the recommendations, it shouldn't be higher than 144.

The causes of such situation are [1, 7, 42]:

- easiness of defining alarms in the design stage with simultaneous problems with removing them (experts arrangements required),
- the occurrence of a large number of alarms in a short period of time in states with serious faults,
- a large number of alarms resulting from a common, single cause (even over 500 alarms),
- repeated alarms (process variables fluctuating close to the alarm threshold),
- lack of proper mechanisms of alarm filtration in the system.

Other disadvantages of AS are long delays in the detection, signalled earlier masking of the symptoms by regulation systems and the lack of automatic fault location. Process operators are then responsible for this task.

Interpretation of a huge number of alarms arising in a short time is a serious problem for the operators, even more that the occurrence of each of the alarms may be caused by various reasons. Here we deal with a phenomenon of information overload, and as a result – stress. In such conditions operators are not able to formulate proper diagnosis, i.e. to recognize the existing risks. It increases the probability of improper protective reactions, the consequences of which, together with previous faults, result in serious accidents. The mechanism of such unfavourable positive feedback was the cause of numerous severe accidents in nuclear and conventional power stations or chemical plants.

The excess of alarms was a cause of accident in Texaco Milford Haven in 1994. During 11 minutes preceding the explosion, 2 operators had to recognize, confirm and properly react to 275 alarms [44].

Nowadays, alarm systems are developed in order to reduce their defects. First of all, they provide mechanisms allowing for the reduction of the number of alarms, such as: filtering the alarms, alarm hiding, alarm shelving and grouping the alarms caused by a common reason. Different algorithms of alarm analysis are also introduced. However, all of these solutions are not able to eliminate all inconveniences resulting from the use of the simplest, but highly deficient method of fault detection, namely limitation control.

2.4. Safety Instrumented Systems (SIS)

SIS is used for implementation of adequate functions of process safety, what allows for achieving proper level of safety integrity [36, 37]. It implements locking and automatic protection algorithms, the aim of which is bringing the process to a safe state. These signals may, for example, cut off power supply or materials inflow, block actuators in a safe position, activate cut-off valves, set safe state of operation of engines, pumps, ventilators etc. Usually, SIS operation is connected with stopping the whole process or a part of it, what results in economic losses.

As regards measurements and control influence, as well as control, SIS should be functionally independent from BPCS control system. This means that security features are realized with the use of devices (usually operating in redundant structure) other than control tasks (Fig. 3). Integration of control and safety systems is permitted at the level of process visualization and configuration tools.

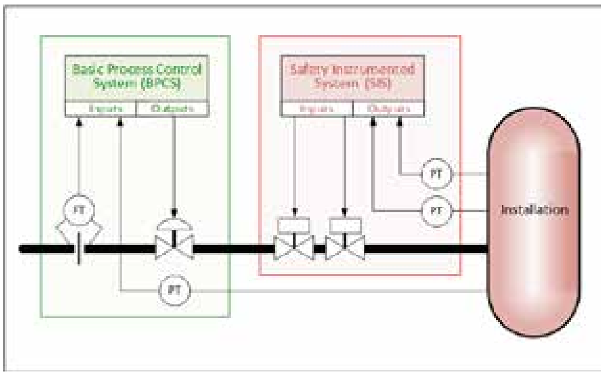
Basic Process Control System (BPCS)
Inputs
Outputs
Safety Instrumented System (SIS)
Inputs
Outputs
FT
PT
PT
PT
PT
Installation

Fig. 3. Separation of BPCS and SIS systems

In SIS we often use a high redundancy level (2oo3, 2oo4D) allowing for achieving appropriate SIL level.

2.5. Higher Layers

These 4 above-mentioned layers aim at preventing accidents. Fifth layer is systems of engineering protection, such as discharge valve, curtains, safety barriers etc., which are only supposed to limit the consequences of the emergencies. The higher layers are protection measures minimizing the results of releases (dikes, security housing), as well as internal and external procedures and technical means, the aim of which is minimizing human and material losses [17].

3. Non-Standard Layers of Protection

Alarm systems due to their faults are not an effective tool for early detection of emergency states. This impedes undertaking effective protective actions by the operators. On the other hand, SIS operation is connected with stopping of the whole process or a part of it leading to economic losses. That is why it is advisable to apply solutions which guarantee elimination of risks in their initial stages and do not allow for SIS activity and emergency system shutdown. The methods of risk reduction, that do not cause stopping of the process are:

- expert real-time diagnostic systems,
- FTCS – Fault Tolerant Control Systems,
- operators training, especially with the use of process simulators, which can run emergency scenarios,
- computer systems for supporting safety – preventing accidents.

These methods are a subject of scientific research and pilot implementation and at this stage are not covered by international regulations.

3.1. Expert Diagnostic Systems

Deficiency of alarm systems is a cause of development of diagnostic systems (DS) for industrial processes. The aim of DS is early detection and recognition of faults (understood as all types of incidents influencing the process in a destructive way), including mainly faults of technological installation components, measuring devices and actuators [6, 12, 15, 16, 18, 29, 28, 24, 25]. Such systems may realize the following functions: faults detection and location, archiving data describing faults, generating diagnostic reports, visualization and justification of diagnoses, supporting operators decisions in emergency states.

In DS intended for industrial processes, the methods of detection using partial models are of basic significance, while these are models designed for a normal state of the process. In Fig. 4 we present

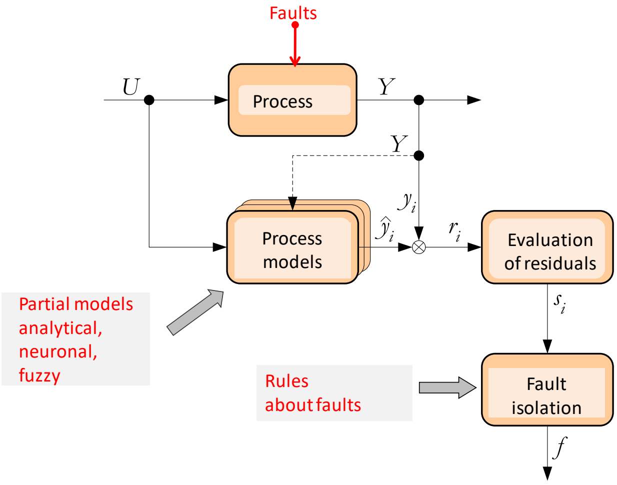

Fig. 4. Diagram of diagnosis with the use of partial model of the process

a diagram of diagnosis with the use of the process models. On the basis of the signals measured and calculated from the model, residues are generated carrying information on the symptoms of the faults (value of the residues diverging from 0) or the lack of them (value of the residues fluctuating around 0). As a result of the residue values assessment, diagnostic signals arise (binary or multiple-valued, crisp or fuzzy), which are the input of an algorithm of fault location. Detection methods based on the models allow for early detection of small faults before their negative consequences appear. Different types of object models can be applied: analytical, neural, fuzzy, statistical [4...15, 18, 28, 6].

Fault location is conducted on the basis of diagnostic signals generated by detection algorithms. The result of location is diagnosis, i.e. hypothesis on the observed fault (faults). For fault location it is necessary to know relation between the values of diagnostic signals S and faults F.

Among the methods of fault location we can distinguish classification methods and automatic inference methods [20]. In fact, in industrial processes there are practically no measurement data for the states of faults. This restricts the possibility of application of classification methods requiring teaching data for particular states of the process. Fault location should then be conducted on the basis of automatic inference and the knowledge on the faults – symptoms relation should be determined on the basis of expert knowledge. The choice of fault detection and location methods is significant for reliable functioning of diagnostic system.

Automatic implementation of diagnostic actions in the course of system operation considerably reduces the time of detection and location of an accident in comparison to diagnostics realized by the alarm system and operator. Diagnoses precisely indicate the observed faults. On this basis, the system is able to additionally advise the personnel by giving instructions to be followed in abnormal and emergency states. Due to that, they can undertake quick and effective protective actions. They should bring the process to a normal state (Fig. 5). As a result, SIS system is not activated and neither the whole technological process nor its part is stopped. Thus we avoid considerable economic losses.

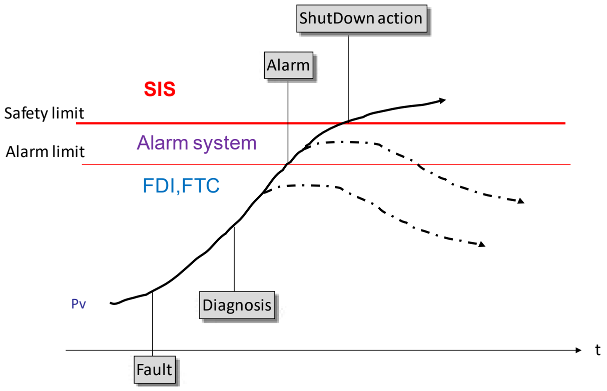

Fig. 5. Courses of the process in the system with and without diagnostics

The beneficial influence of the diagnostics performed in real time on the reliability and security of the system may be proved by analysing the indicators characterizing these properties. For correctable systems it is common to use availability factor of the system. It is expressed by the following formula:

$$A = \frac{T_\lambda}{T_\lambda + T_\mu} = \frac{\mathrm{MTTF}}{\mathrm{MTBF}} \qquad (1)$$

where:

- MTTF – Mean Time To Failure – T_λ,
- Mean Time Between Failures – MTBF = MTTF + MTTR.
- MTTR – Mean Time To Repair, i.e. mean time from the moment of diagnosing failure to the moment of repairing the damaged equipment – T_μ,
- Mean Time To Diagnose – T_D,
- Mean Time to Renewal, i.e. repairing the damaged equipment or replacing it with a suitable one together with reconstruction of the system after the repair/replacement – T_N.

Mean Time To Repair is the sum of Mean Times To Diagnose and Replacement of the device:

$$T_\mu = T_D + T_N \qquad (2)$$

Shortening diagnostic times reduces the time T_μ (MTTR), thus increasing the value of availability factor of the system (1). In practice, the time of diagnosis realized automatically is close to 0: $T_D \approx 0$.

Intensity of the damages is the reverse of the mean time to the fault:

$$\lambda = \frac{1}{T_\lambda} \qquad (3)$$

The total intensity (probability) of the faults λ is the total of the intensities of dangerous detectable faults λ_{DD}, dangerous undetectable faults λ_{DU}, safe detectable faults λ_{DS} and safe undetectable faults λ_{SU} [36]:

$$\lambda = \lambda_{DD} + \lambda_{DU} + \lambda_{SD} + \lambda_{SU} \qquad (4)$$

Safety Integrity Level (SIL) specified in EN 61508 norm [36] depends on: the mean probability of not fulfilling the security function (PDF_{SYS}) – for security systems operating for call or mean probability of a dangerous fault per hour (PFH_{SYS}) – for security systems operating in a continuous manner. The values of these probabilities depend, inter alia, on DC diagnostic coverage, which is formulated as follows:

$$DC = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}} \tag{5}$$

Formula (5) shows that covering all dangerous faults by current diagnostics allows for increasing diagnostic coverage factor to the value of 1. This will reduce the risk, i.e. limit PDF_{SYS} lub PFH_{SYS}.

Another factor exemplifying the influence of diagnostics is SFF (Safe Failure Fraction) factor determining contribution of the safe faults:

$$SFF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}} = \frac{\lambda - \lambda_{DU}}{\lambda} \tag{6}$$

The more faults is detected the higher the value of this factor, and with full detectability it is equal to 1. This factor is of crucial importance for SIL verification of E/E/PE system made on the basis of data on the tolerance of the equipment faults.

Example 1. Comparison of the operation of alarm and diagnostic systems

Below can be found an example of alarm and diagnostic system for a simple installation of buffer tank of a toxic substance. Diagram of the object, as well as the system of level regulation, is presented in Fig. 6.

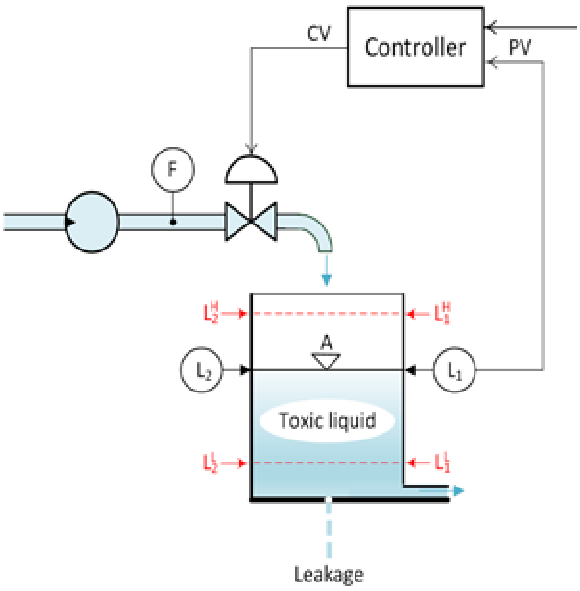

Fig. 6. Diagram of the object – buffer tank of toxic substance and level control system

In the alarm system, alarms L_{1LO}, L_{1HI}, L_{2LO}, L_{2HI}, L_{LO} are detected. On the basis of the exceeded values of limiting the bottom of medium in the tank with the normal value of the F flow, operator may infer that the f_1 fault has occurred – leak in a tank and leak of toxic medium. Inference algorithm is as follows:

$$If\left(L_{1LO} \wedge L_{2LO} \wedge \neg F_{LO}\right) Then\ f_1 \tag{7}$$

Diagnostic system for the analysed object performs the following four tests:

$$r_1 = F - \alpha_{12} S \sqrt{2gL_1} - A\frac{dL_1}{dt}, \tag{8}$$

$$r_2 = F - \alpha_{12} S \sqrt{2gL_2} - A\frac{dL_2}{dt}, \tag{9}$$

$$r_3 = F - \hat{F} = F - f\left(CV\right) \tag{10}$$

$$r_4 = L_1 - L_2. \tag{11}$$

Test 1 and test 2 detects faults on the basis of non-compliance of the balance in the tank. Test 3 controls the compatibility of the measured flow and flow calculated from the model of the control valve $\hat{F} = f\left(CV\right)$. The model of water flow through the control valve has only one input – the CV signal from the controller. In the general case, such flow is also dependent on the pressure difference on the valve. However in this case it can be concluded that such drop is approximately constant. Well-adjusted pump should ensure the stability of pressure in front of the valve in the whole range of flow changes, whereas behind the valve the liquid flows out freely and at the end of the pipeline pressure is equal to atmospheric pressure. Therefore, the difference in pressures at the valves is constant. Test 4 verifies the compatibility of redundancy measurements of the medium level in the tank. Table 1 summarizes the possible faults.

Tab. 1. List of faults

Symbol	**Fault**
f_1	leak of a toxic substance
f_3	damage to the control valve
f_3	damage to F measurement chain
f_4	damage to L1 measurement chain
f_5	damage to L2 measurement chain

The sensitivity of the particular tests on faults is given in binary diagnostic matrix (Tab. 2).

Tab. 2. Binary diagnostic matrix for buffer tank

S/F	f_1	f_2	f_3	f_4	f_5
s_1	1		1	1	
s_2	1		1		1
s_3		1	1		
s_4				1	1

According to binary diagnostic matrix, all faults are detectable in the designed diagnostic system. Leak of toxic substance is detected on the basis of the following principle:

$$If\left(s_1 = 1\right) \wedge \left(s_2 = 1\right) \wedge \left(s_3 = 0\right) \wedge \left(s_4 = 0\right) Then\ f_1 \tag{12}$$

Comparing the operation of the alarm system with a diagnostic system one can state that:

- in the alarm system the leak may stay undetected due to masking effect of the control circuit – detection is uncertain,
- inferring on the causes of the alarm, according to dependency (7) is conducted by the operator, what may cause additional delays. Delays in inferring may also depend on the difference between the value of medium level in the moment of a failure and lower limit LO LIMIT;
- time to recognize the toxic substance is definitely faster in the case of diagnostic system. It depends on the accepted residue limitations (they can be sharp or fuzzy), but automatic recognition of the fault is fast and reliable.

3.2. Fault Tolerant Control System

Diagnostics realized in a real time is also the basis for realization of Fault Tolerant Control (FTC) systems [4, 9, 16, 18, 34, 10, 3]. FTC systems are currently one of the most important directions of research and development as regards automatic control. First works from this range concerned aviation industry. However, nowadays, in addition to applications in aircraft, FTC systems are designed in industrial processes.

The idea of active FTC systems design consists in the realization of current diagnostics and real-time re-configuration of the equipment or program structure of the system in the states with faults. Instead of operator intervention, restoring the ability of the system functioning is automatic. Therefore, these are systems of variable structure. The general diagram of Fault Tolerant Control system is presented in Fig. 7.

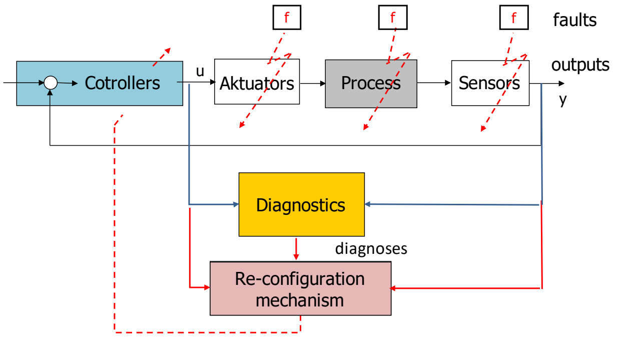

Fig. 7. The diagram of FTC system (u - control signals, y – outputs, f – faults)

The concept of FTC systems itself coincides with the structure of dynamic redundancy. Specific nature of FTC systems is the use of program redundancy instead of equipment redundancy. When designing FTC systems, mainly measurement and actuator devices' faults are taken into consideration. To recognize faults of the elements of the control system, diagnostic methods are applied based on the process models.

In complex control systems, even with no equipment redundancy, there are usually possible re-configurations of automatic systems in such a way to eliminate or reduce the unfavourable influence of the damages to the measuring circuits on the functioning of the process. In order to reproduce the values of the signals, which measuring circuits are damaged we usually use virtual sensors, which calculate the value of the signal on the basis of the model, using other measurement signals. Dynamic substitution of signal values from the damaged measuring circuits by equivalent signals is also possible.

Much more difficult is to design systems resistant to faults of actuators. In the case of multidimensional objects with numerous control inputs, the inability to change the value of one of the inputs may be in some cases neutralized by appropriate setting of the remaining inputs. As an example, damage to the single engine in a plane may be compensated by changes of flying qualities, deflecting flaps and skilful power dispense of other engines. However, in most cases redundancy of these devices is indispensable.

Developing Fault Tolerant Control system requires designing for each of the faults an algorithm of automatic system functioning in the state of this fault and the procedure of non-impact switching from the normal state control to reserve control. The condition for making such changes is however adequately quick detection and unambiguous location of the faults.

Research works in the field of FTC systems are focused on the advanced control systems, while more than 90% of all applications are the systems with PID controllers [26]. This is the cause of delays of the current state of the art in relation to the progress in scientific research. The current control systems only marginally allow for designing systems tolerant of faults, as they are not equipped with the appropriate diagnostic and re-configuration software. FTC systems' applications have the character of research and pilot implementations.

Example 2. Level control system of the boiler drum in sugar-refinery tolerating faults of measurement chains

Control of the water level in a boiler drum of sugar-refinery is led in a cascade structure, when the main value of control is the level and supporting role is given to the inflow of supplying water and steam outflow. Tolerating faults of the L_1, F_1, F_2 measurement chains is realized with the use of virtual sensors of these physical quantities executed in the technique of neural networks. Virtual sensor of the water level of a $\hat{L}_3 = f(F_1,F_2,P_2)$ structure is only required to provide reliable fault diagnosis of the faults of L_1 and L_2 equipment chains. When L_1 chain is damaged switching into redundancy L_2 equipment chain is performed, provided that it is fit. When diagnostic system detects fault in measurement chain of F_1, F_2 water or steam flow, appropriate virtual sensor is used: $\hat{F}_1 = f(Y_1,P_1,P_2)$ lub $\hat{F}_2 = f(P_2,P_3,Y_2)$. To detection and localization of faults, diagnostic systems use all three aforementioned models and other simple relations between process variables.

In faults tolerated by control systems, both, time of diagnostics realized automatically is close to zero: $T_D \approx 0$, and time of automatically executed re-configuration is reduced to zero $T_N \approx 0$. This increases system's availability $A \approx 1$.

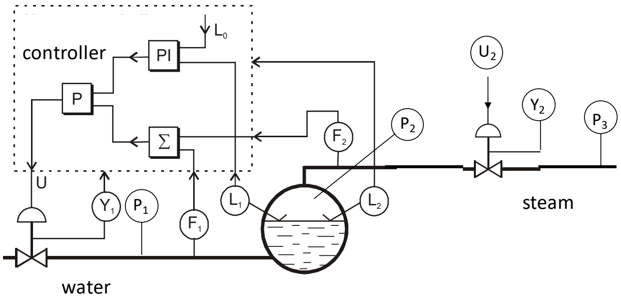

Fig. 8. The structure of the level control system in boiler drum in sugar-refinery tolerating faults of measurement chains. Symbols: L_1, L_2 – measurements of the water level in boiler drum, F_1 – inflow of water supplying boiler, F_2 – steam outflow, P_1- pressure of supplying water, P_2 – pressure in boiler drum, P_3 – steam pressure at the outlet (behind control valve), Y_1 – location of the piston rod on the water inflow, Y_2 – location of the piston rod on the steam outflow

PFH_{SYS} probability for the entire FTC control system is determined by the following formula:

$$PFH_{SYS} = PFH_I + PFH_C + PFH_A \qquad (13)$$

where particular elements correspond to the mean probability of dangerous fault per hour for the measurements of a controller and actuator. Due to the fact of tolerating faults of all measurement chains, $PFH_I \approx 0$ and thus the value of PFH_{SYS} for the entire system decreases.

The above mentioned example shows that implementation of the control systems tolerating faults significantly contributes to the improvement of security and reliability of control systems and controlled processes.

3.3. Process Simulators

Statistical information on the causes of all types of damages from different sources are rather similar and indicate human errors as the most frequent cause (about 40%). The basic method of human errors reduction is training. Process operators perform particularly significant role. They analyse the alarms and make crucial decisions on the way of conducting the process in abnormal states.

Requirements concerning adequate preparation of operators is particularly difficult to fulfil, since we notice that together with the increase of the level of automation and reliability of the process installation, operators qualifications in the area of undertaking proper actions in unusual and emergency situations are getting worse. They rarely conduct the process in the mode of manual control and thus they don't feel its dynamics. Moreover, training of operators at real and operating installation is ineffective mainly due to the inability to train reactions in abnormal and emergency states. Even during the longest period of training all possible states of installation operation hardly ever happen, what sooner or later result in a situation when an operator will have to work in conditions he was not prepared to work (as an example, fault which didn't occur during the training).

Avoiding all mentioned inconveniences is possible due to the application of program simulators of processes coupled with the real control system. Simulators are realized on the basis of equations describing physical phenomena occurring in the object. Differential equations describing the object are in many cases very complex, there can occur highly non-linear relations with distributed parameters etc. Solving such set of equations with the use of numerical methods requires high computational costs and does not guarantee the realization of calculations in a real time. That is why we commonly use approximation models for building simulators, which has to reproduce the functioning of a real object with proper accuracy [15].

Requirements placed for process simulators are very strict. They have to, among others:

- reproduce different states of the process, particularly: different points of operation, load changes, start and withdrawal,
- ensure a possibility of simulating emergency states,
- ensure a possibility of tuning parameters in order to obtain satisfactory compliance with the real process,
- cooperate with physical control system or emulate this system with its protection system.

Simulator of the process developed for the purposes of operators training may be later used for process diagnostics, testing new strategies of control and optimization of the object operation.

3.4. Security Support Systems – Preventing Accidents

Significant element of supporting security in the facilities of increased or high risk may be computer systems preventing accidents. Their aim is to gather in a database documentation concerning safety, as well as monitoring and supervising actions connected with counteracting threats. The need of their realization results from legal regulations imposing a number of obligations on the industrial plants, as well as on the supervisory bodies. These are: Environmental Protection Law and the Directive 2012/18/EU of the European Parliament and Council on the control of major accident hazards involving dangerous substances. According to these regulations, one of the most important procedures of the system of counteracting serious accidents is a system of safety management (SSM), which implements a program of accident prevention (PAP) in the facility. Exemplary solution of such system is presented in Chapter 4.

4. Intelligent Accident Prevention System IAPS

Developing this system was undertook by the Institute of Automatic Control and Robotics of Warsaw University of Technology. The aim of the project is realization of IAPS – Intelligent Accident Prevention System. This is a computer system supporting introduction and monitoring of safety systems in facilities posing a risk of serious industrial accident. The operation of the system consists in gathering digital documentation connected with safety in the plant, monitoring and supervising tasks connected with implementation and realization of SSM and PAP, as well as supporting making and gathering of data in the field of risk analysis, including HAZOP (Hazard and Operability Study). The system enables gathering in digital version and providing to the authorized people in a plant, as well as external entities, such as State Fire Service units, Chief Environmental Protection Inspectorate, Office of Technical Inspection, any data and documentation concerning safety in a plant, among others – a list of hazardous substances that can be found in a plant, the results of risk and emergency situations analyses, operational and rescue plans etc. The use of the system means introducing a new generation of tools supporting safety systems in facilities posing a risk of serious industrial accidents. Such solution should contribute to the increase of safety and competitiveness of all companies which will implement the system. It will be an additional security layer, the aim of which is prevention activities, securing against the occurrence of serious industrial accident. Such actions are of organizational character and include gathering and clearing the documentation connected with safety in a plant, as well as monitoring the current tasks concerning counteracting serious industrial accidents. The system enables also remote supervision of the plant by the authorized institutions.

5. Conclusion

The paper points out that not only the SIS influences the safety of the process, but the risk reduction may also be achieved by the use of:

- the system of current diagnostics of process and object devices
- fault tolerant control systems
- process simulators for the purposes of operators training
- computer systems of accident prevention

Diagnostic systems together with the operators interventions, as well as FTC systems may constitute additional layer of protection for the process [19]. It reduces process risk by eliminating threats in their early stage. At the same time it reduces economic losses in the states of fault, because it does not lead to stopping of the process and thus – production.

Diagnostic systems for industrial processes, as well as fault tolerant control systems are not sufficiently widespread in industry, but they are in the stage of pilot research and first implementations. We can expect that in a short time there will be an intense development of control systems equipped with software for process diagnostics and realization of FTC systems, as well as an increase in the number of industrial applications in this area. A certain obstacle impeding industrial applications is the lack of specialists in this field. However, at the moment at many universities these issues are included in the curriculum and young engineers will get prepared to the realization of innovative solutions of control systems. Additional argument supporting its application is striving for the reduction of economic losses connected with the faults and the ability to reduce the insurance costs of technological installation.

Simulators are commonly used for the training of pilots, captains and operators in nuclear power stations. They are more and more frequently used also in conventional power sector and petrochemical and chemical industry. We may expect a rapid growth of their applications, despite high costs of their construction. Increasing number of companies offer simulators dedicated to specific processes. There are also program packages which are the basis for realization of the simulators. Introducing training on the simulators will result in significant increase of safety of the process and reduction of economic losses caused by the operators errors.

Computer systems of accident prevention have a significant impact on the organizational part in the facilities of increased or high risk. Gathering and organizing the documentation connected with safety in a plant in a digital form and monitoring of current tasks concerning counteracting serious industrial accidents significantly influences the quality of organizational activities, human competences and increase of safety culture. Such system also allows for manual supervision of the plant by the authorized institutions.

Acknowledgements

Developed on the basis of the results of the 3rd stage of the long-term program entitled “Improving the safety and working conditions” funded by the Ministry of Science and Higher Education/National Centre for Research and Development in the years 2014-2016 in the field of research and development.

Coordinator of the program: Central Institute for Labour Protection – National Research Institute.

AUTHOR

Jan Maciej Kościelny – Warsaw University of Technology, Faculty of Mechatronics, Institute of Automatic Control and Robotics, ul. Św. Andrzeja Boboli 8, 02-525, Poland, E-mail: jmk@mchtr.pw.edu.pl
Michał Syfert – Warsaw University of Technology, Faculty of Mechatronics, Institute of Automatic Control and Robotics, ul. Św. Andrzeja Boboli 8, 02-525, Poland, E-mail: m.syfert@mchtr.pw.edu.pl
Bartłomiej Fajdek* – Warsaw University of Technology, Faculty of Mechatronics, Institute of Automatic Control and Robotics, ul. Św. Andrzeja Boboli 8, 02-525, Poland, E-mail: b.fajdek@mchtr.pw.edu.pl

*Corresponding author

REFERENCES

[1] J. Errington, D. V. Reising, C. Burns, and ASM Joint R & D Consortium, *Effective alarm management practices*, ASM Consortium: Phoenix, 2009.

[2] S. Bajpai and J. P. Gupta, “Terror-Proofing Chemical Process Industries”, *Process Safety and Envi-*

ronmental Protection, vol. 85, no. 6, 2007, 559–565
DOI: 10.1205/psep06046.

[3] M. Blanke, C. Frei, F. Kraus, R. J. Patton, and M. Staroswiecki. "Fault-tolerant Control Systems". In: K. Åström, P. Albertos, M. Blanke, A. Isidori, W. Schaufelberger, and R. Sanz, eds., *Control of Complex Systems*, 165–189, Springer London, 2001.

[4] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and Fault-Tolerant Control*, Springer-Verlag: Berlin Heidelberg, 2006.

[5] J. Chen and R. J. Patton, *Robust Model-Based Fault Diagnosis for Dynamic Systems*, The International Series on Asian Studies in Computer and Information Science, Springer US, 1999.

[6] J. Chen and R. Patton, *Robust Model-Based Fault Diagnosis for Dynamic Systems*, Springer, 2012.

[7] Engineering equipment and materials users association EEMUA Publication 191: *Alarm Systems – A Guide to Design, Management & Procurement*, London, 2007.

[8] J. Gertler, *Fault detection and diagnosis in engineering systems*, Marcel Dekker: New York, 1998.

[9] R. Isermann, *Fault-diagnosis systems: an introduction from fault detection to fault tolerance*, Springer: Berlin; New York, 2006.

[10] J. Jiang and X. Yu, "Fault-tolerant control systems: A comparative study between active and passive approaches", *Annual Reviews in Control*, vol. 36, no. 1, 2012, 60–72
DOI: 10.1016/j.arcontrol.2012.03.005.

[11] C. Jochum, "Can Chemical Plants be Protected Against Terrorist Attacks?", *Process Safety and Environmental Protection*, vol. 83, no. 5, 2005, 459–462
DOI: 10.1205/psep.04189.

[12] S. Kabir, M. Walker, Y. Papadopoulos, E. Rüde, and P. Securius, "Fuzzy temporal fault tree analysis of dynamic systems", *International Journal of Approximate Reasoning*, vol. 77, 2016, 20–37
DOI: 10.1016/j.ijar.2016.05.006.

[13] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security". In: *IECON 2011 – 37th Annual Conference of the IEEE Industrial Electronics Society, Melbourne*, 2011, 4490–4494
DOI: 10.1109/IECON.2011.6120048.

[14] F. Khan, S. Rathnayaka, and S. Ahmed, "Methods and models in process safety and risk management: Past, present and future", *Process Safety and Environmental Protection*, vol. 98, 2015, 116–147
DOI: 10.1016/j.psep.2015.07.005.

[15] J. Korbicz and J. M. Kościelny, eds., *Modeling, diagnostics and process control: implementation in the DiaSter system*, Springer-Verlag: Berlin, Heidelberg, 2010.

[16] J. Korbicz, J. M. Kościelny, Z. Kowalczuk, and W. Cholewa, eds., *Diagnostyka procesów: modele, metody sztucznej inteligencji, zastosowania, (Diagnostics of processes: models, artificial intelligence methods, applications)*, Wydawnictwa Naukowo-Techniczne: Warszawa, 2002 (in Polish).

[17] K. T. Kosmowski, ed., *Podstawy bezpieczeństwa funkcjonalnego (Basics of functional safety)*, Wydawnictwo Politechniki Gdańskiej: Gdańsk, 2016 (in Polish).

[18] J. M. Kościelny, *Diagnostyka zautomatyzowanych procesów przemysłowych (Diagnostics of automated industrial processes)*, Akademicka Oficyna Wydawnicza EXIT: Warszawa, 2001 (in Polish).

[19] J. M. Kościelny and M. Bartyś, "The Requirements for a New Layer in the Industrial Safety Systems". In: *IFAC-PapersOnLine*, vol. 48, Paris, France, 2015, 1333–1338
DOI: 10.1016/j.ifacol.2015.09.710.

[20] S. Leonhardt and M. Ayoubi, "Methods of fault diagnosis", *Control Engineering Practice*, vol. 5, no. 5, 1997, 683–692
DOI: 10.1016/S0967-0661(97)00 050-6.

[21] E. K. Mihailidou, K. D. Antoniadis, and M. J. Assael, "The 319 Major Industrial Accidents Since 1917", *International Review of Chemical Engineering*, vol. 4, no. 6, 2012, 529–540.

[22] T. Missala, *Analiza wymagań i metod postępowania przy ocenie ryzyka i określaniu wymaganego poziomu nienaruszalności bezpieczeństwa (Analysis of requirements and proceeding methods for risk evaluation and determining the required safety integrity level)*, Oficyna Wydawnicza PIAP: Warszawa, 2009 (in Polish).

[23] P. Okoh and S. Haugen, "A study of maintenancerelated major accident cases in the 21st century", *Process Safety and Environmental Protection*, vol. 92, no. 4, 2014, 346–356
DOI: 10.1016/j.psep.2014.03.001.

[24] Y. Papadopoulos, "Model-based system monitoring and diagnosis of failures using statecharts and fault trees", *Reliability Engineering & System Safety*, vol. 81, no. 3, 2003, 325–341
DOI: 10.1016/S0951-8320(03)00095-4.

[25] R. J. Patton, P. M. Frank, and R. N. Clark, eds., *Issues of Fault Diagnosis for Dynamic Systems*, Springer-Verlag: London, 2000.

[26] M. Pawlak, J. M. Kościelny, and P. Wasiewicz, "Method of increasing the reliability and safety of the processes through the use of fault tolerant control systems", *Eksploatacja i Niezawodnosc – Maintenance and Reliability*, vol. 17, no. 3, 2015, 398–407
DOI: 10.17531/ein.2015.3.10.

[27] E. Piesik, M. Śliwiński, and T. Barnert, "Determining and verifying the safety integrity level of the safety instrumented systems with the uncertainty and security aspects", *Reliability Engineering & System Safety*, vol. 152, 2016, 259–272
DOI: 10.1016/j.ress.2016.03.018.

[28] S. Simani, C. Fantuzzi, and R. J. Patton, *Model-based Fault Diagnosis in Dynamic Systems Using Identification Techniques*, Advances in Industrial Control, Springer-Verlag: London, 2003.

[29] M. Syfert, P. Wnuk, and J. M. Kościelny, "DiaSter – Intelligent system for diagnostics and automatic control support of industrial processes", *Journal of Automation, Mobile Robotics and Intelligent Systems*, vol. 5, no. 4, 2011, 41–46.

[30] P. Tatjewski, J. M. Kościelny, W. Nagórko, and L. Trybus. "Wybrane układy i systemy automatyki przemysłowej: systemy sterowania, sterowanie zaawansowane, diagnostyka, zarządzanie alarmami (Selected schemes and control systems of industrial automation: control systems, advanced control, diagnostics, alarm management)". In: K. Malinowski and R. Dindorf, eds., *Postępy automatyki i robotyki*, volume 2, 350–

382. Wydawnictwo Politechniki Świętokrzyskiej, Kielce, 2011 (in Polish).

[31] T. Barnert, K. Kosmowski and M. Śliwiński, "Security Aspects in Verification of the Safety Integrity Level of Distributed Control and Protection Systems", *Journal of KONBiN*, vol. 6, no. 3, 2008, 25–40 DOI: 10.2478/v10040-008-0056-0.

[32] L. Urbas, A. Krause, and J. Ziegler, *Process control systems engineering*, Oldenbourg Industrieverl: München, 2012.

[33] H.-J. Uth, "Trends in major industrial accidents in Germany", *Journal of Loss Prevention in the Process Industries*, vol. 12, no. 1, 1999, 69–73 DOI: 10.1016/S0950-4230(98)00039-4.

[34] M. Mahmoud, J. Jiang, and Y. Zhang, *Active Fault Tolerant Control Systems: Stochastic Analysis and Synthesis, Lecture Notes in Control and Information Sciences*, Springer-Verlag: Berlin Heidelberg, 2003.

[35] E. Zio and T. Aven, "Industrial disasters: Extreme events, extremely rare. Some reflections on the treatment of uncertainties in the assessment of the associated risks", *Process Safety and Environmental Protection*, vol. 91, no. 1, 2013, 31–45 DOI: 10.1016/j.psep.2012.01.004.

[36] Technical Standard: "PN-EN 61508: Bezpieczeństwo funkcjonalne elektrycznych / elektronicznych / programowalnych elektronicznych systemów związanych z bezpieczeństwem (Functional safety of electrical / electronic / programmable electronic safety-related systems)", *PKN*, Warszawa, 2003 (in Polish).

[37] Technical Standard: "PN-EN 61511: Bezpieczeństwo funkcjonalne. Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego (Functional safety. Safety instrumented systems for the sector of process industry)", *PKN*, Warszawa, 2005 (in Polish).

[38] Technical Standard: "IEC 61508, Functional safety of electrical/ electronic/programmable electronic safety-related systems", *International Electrotechnical Commission*, 1998.

[39] Technical Standard: "IEC 61511, Functional safety – Safety instrumented systems for the process industry sector", *International Electrotechnical Commission*, 2003.

[40] Technical Standard: "IEC 62061, Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems", *International Electrotechnical Commission*, 2005.

[41] Technical Standard: "IEC 61513, Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems", *International Electrotechnical Commission*, 2001.

[42] "ANSI/ISA-18.2, Management of Alarm Systems for the Process Industries", *ISA 18 Committee*, 2009.

[43] Crescenzi F. et al.,"Vessel and In-Vessel Components Design Upgrade of the FAST Machine", Fusion Engineering and Design 88 (9-10), pp. 2048-2051, 2013.

[44] Health and Safety Executive, *The explosion and fire at the Texaco refinery, Milford Haven, 24 July 1994: a report of the investigation by the Health and Safety Executive into the explosion and fires on the Pembroke Cracking Company Plant at the Texaco Refinery, Milford Haven on 24 July 1994.*, HSE Books: Sudbury, 1997.